On Data Security Protection Strategies for Petrochemical Enterprises amidst the Era of Big Data

Aijiao Jing[1,a], Liang Song[b*], Qi Chen[1,c], Xinbei Lv[1,d], Huanyu Zhou[1,e]

[1]Digital Intelligence Company, PetroChina Southwest Oil & Gasfield Company, Chengdu, China
[2]Sichuan Energy Internet Research Institute, Tsinghua University, Chengdu, China

[a]jingaijiao@petrochina.com.cn
b*Corresponding author:songliang@tsinghua-eiri.org
[c]chen.qi@petrochina.com.cn;[d]lxb1997@petrochina.com.cn
[e]zhouhuanyu@petrochina.com.cn

Abstract. Amidst the era of big data, data is not only a crucial asset for countries and businesses but also a key driver for economic and social development as well as innovation in management mechanism. Any occurrence of data security issues can lead to significant losses for countries, enterprises, and individuals, resulting in substantial social impact. Therefore, it is highly important to conduct thorough research on data security protection strategies for petrochemical enterprises. This paper first analyzes the risks associated with data security under the backdrop of big data and proposes a framework for designing data security protection strategies based on the Data Security Capability Maturity Model. The framework consists of two main components: management framework design and technical framework design. This paper primarily focuses on studying the design of the technical framework. By conducting targeted risk analysis throughout the entire lifecycle of data including acquisition, transmission, storage, application, sharing, and destruction stages; it aims to align each identified risk with corresponding measures for ensuring data security protection. Additionally, this paper suggests protection strategies tailored to enterprise scenarios dimensions to provide robust security guarantees for petrochemical enterprise's valuable datasets.

Keywords: Petrochemical enterprises; Data security risk; Data security protection strategy; Dimension of enterprise scenarios

1 Introduction

Amidst the era of rapid big data development, security concerns have become increasingly important. Big data security risks can result in significant losses, highlighting the need for robust protection measures. While there has been progress in data security technology, challenges remain such as insufficient research and development efforts towards technical means and delayed initiation of data security technology

B. K. Kandel et al. (eds.), *Proceedings of the 2023 8th International Conference on Engineering Management (ICEM 2023)*, Atlantis Highlights in Engineering 23,
https://doi.org/10.2991/978-94-6463-308-5_14

research [1]. To establish a new ecosystem for big data applications with high information sharing and stringent security guarantees, it is necessary to strengthen the foundation of big data application's security while enhancing standardized management capabilities and systematic protective measures [2-3].

2 Data Security Risks

With the increasing integration and application of the Internet in the petrochemical sector, data security risks for petrochemical enterprises are becoming more prominent under complex and severe security situations. As a crucial factor to ensure digital transformation and development of enterprises, data security for petrochemical entities must be given first priority.

Risks associated with log collection. In the process of secured access, real-time collection of equipment, application, service and other related logs, alarms and data is necessary to provide background support for security monitoring and analysis.

User access risks arise from incorrect user identity authentication and exceeding access limits. In a zero-trust system, users must be authenticated by the authentication service and their identities continuously verified during the access process to ensure credibility. Cross-network user access should use VPN technology to reach data resources through a virtual desktop, with environment awareness services sensing terminal security status for secure access [4]. The data access risks manifest in the following two aspects: firstly, there exists a deviation in user identity authentication, enabling unauthorized users to gain access to the cloud platform and resulting in data theft; secondly, subsequent to legitimate user identity authentication, excessive access occurs which leads to data leakage [5-6].

Risks from transmission encryption and decryption. In the context of data transmission, there exists a potential risk [7] when utilizing network transmission encryption services within the security protection system to encrypt communication links, ensuring confidentiality and integrity during the process of transmitting data. However, it is essential to decrypt encrypted traffic for effective security detection while monitoring network traffic.

Access control risks. Access control can be categorized into network access control, application access control, service access control, and data access control. During the process of user accessing application data resources, comprehensive monitoring and auditing of network attacks, user behavior, and network risks are conducted to achieve the protection objectives of big data security, trustworthiness, and compliance [8].

Data sharing risk. Data sharing poses a risk, as the flow of data is crucial in unlocking its value. Static and isolated data may struggle to fulfill its potential, while also introducing new security risks. Internet infrastructure operators, system integrators, security vendors, and data exchanges [9] face challenges in determining the rights and responsibilities of data ownership, hindering effective implementation of industrial internet protection measures. Additionally, tracking the flow of data can be difficult

without adequate technical means to monitor processing activities by receivers who may engage in illegal use [10-11].

Data destruction risk in cloud computing environments arises due to the complexity of data encryption and multiple backups. During data destruction operations, original data is mostly destroyed while backup data remains unprocessed, making it vulnerable to theft by criminals and posing a threat to enterprise interests and personal rights. This leads to potential risks of data destruction.

3 Design of Data Security Protection Strategy Framework

This study focuses on the data life cycle, with a central emphasis on data security protection strategies in petrochemical enterprises. It provides specific implementation guidelines [12-14] from both management and technological perspectives, aiming to offer valuable insights for enhancing data security protection. The formulation of these strategies is based on the *Information Security Technology—Data Security Capability Maturity Model* (GB/T 37988-2019), tailored to suit the enterprise's actual circumstances.

The establishment of a robust information security system by the enterprise indicates that data security is not an isolated endeavor. It encompasses comprehensive measures implemented within the information system and network environment to ensure in-depth protection at various levels. These efforts primarily revolve around enhancing information and network security, with due consideration given to safeguarding data integrity.

3.1 Protection Requirements

The enterprise data security protection strategy is designed by referencing the *Information Security Technology—Data Security Capability Maturity Model* (GB/T37988-2019), which encompasses the data security protection requirements of the process domain (as shown in Table 1).

Table 1. Data Security Protection Requirements of the Data Security Capability Maturity Model

Stages	Processes	Specific Contents	Remarks
Data Acquisition	Data acquisition security management	In the process of collecting data from external customers, partners, and other relevant parties, the organization should clearly define the purpose and utilization of data acquisition. It is essential to ensure the authenticity, effectiveness, and adequacy of the data source while also specifying the channels for data acquisition. Standardizing the format of acquired data along with related processes and methods is crucial to guarantee compliance, legitimacy, and consistency.	
	Identification and recording of data sources	Identification and documentation of data sources to mitigate the risks of data phishing and forgery.	
	Data quality management	Reinforce the establishment of an organizational data quality management system to ensure the precision, coherence, and integrity of the data collected/generated throughout the process of data acquisition.	

Data Transmission	Encryption of data transmission	Adopt appropriate encryption measures in accordance with the internal and external data transmission requirements of the organization to ensure secure transmission channels, nodes, and data, thereby preventing any potential leakage during transmission.	
	Network availability management	By implementing network infrastructure backup and deploying data leakage prevention equipment at the network layer, we aim to achieve optimal network availability, thereby ensuring the utmost stability in the process of data transmission.	
Data Storage	Storage media security	To provide effective technical and managerial measures for scenarios that require access to and use of data storage media within the organization, in order to prevent the risk of data leakage resulting from improper media usage. Storage media encompasses both terminal devices and network storage.	
	Logical storage security	Develop robust security measures for data logical storage, storage containers, etc., based on the organizational business characteristics and data storage security policies to ensure effective implementation.	
	Data backup and recovery	The achievement of redundant data management and protection of data availability are ensured through the implementation of regular data backup and recovery.	
Data Application	Data desensitization	Data import and export security	
	Data analysis security	By implementing appropriate security control measures during the data analysis process, we can effectively mitigate the potential security risks associated with valuable information and personal privacy leakage in data mining and analysis.	
	Proper use of data	In accordance with relevant national laws and regulations governing data analysis and utilization, a mechanism for responsibility and evaluation of the data usage process must be established to safeguard state secrets, trade secrets, personal privacy, and prevent improper use of data resources.	
	Security of data processing environment	Establish a security protection mechanism for the data application environment within the organization, providing a unified platform for data calculation and development, while ensuring complete management of security controls and technical support throughout the process of data application.	
	Data import and export security	The management of data security during the process of data import and export can effectively mitigate potential risks to data availability, integrity, and leakage.	
Data Sharing	Data sharing security	The implementation of security risk control occurs when data is shared with external organizations through business systems or products, as well as during data exchange with partners in collaborative efforts, aiming to mitigate security risks associated with data sharing scenarios.	
	Data distribution security	In the process of data disclosure to external organizations, it is imperative to exercise control over the format, applicability scope, rights and obligations of publishers and users in order to ensure the security, manageability, and compliance of data throughout its release.	
	Data interface security	By implementing a security management mechanism for the external data interface of an organization, it is possible to mitigate the potential security risks associated with invoking interfaces and ensure the protection of organizational data.	
Data Destruction	Data destruction disposal	By implementing a mechanism for data deletion and purification, effective destruction of data is achieved, thereby mitigating the risk of data leakage resulting from recovery of residual data on storage media.	
	Storage media destruction disposal	By establishing robust procedures and employing advanced technological measures for the secure destruction of storage media, this study aims to mitigate the security risks associated with data leakage resulting from loss, theft, or unauthorized access to such media..	
	Data supply chain security	By implementing an effective data supply chain management mechanism, the organization can mitigate security risks associated with its upstream and downstream data supply processes.	
	Terminal data security	The terminals within the organization should adopt appropriate technical and management plans in accordance with the organization's require-	

		ments for data protection at the terminal equipment level.	
	Monitoring and auditing	Conduct comprehensive security monitoring and auditing throughout all stages of the data life cycle to ensure effective surveillance and auditability of data access and operations, thereby achieving prevention and control of unauthorized access, data misuse, data leakage, and other potential security risks inherent in every phase of the data life cycle.	

3.2 Design Basis

Data security entails numerous standards and intricate application scenarios. Prior to devising a framework for protection policies, it is imperative to sort out and clarify the design concepts, as depicted in Figure 1.

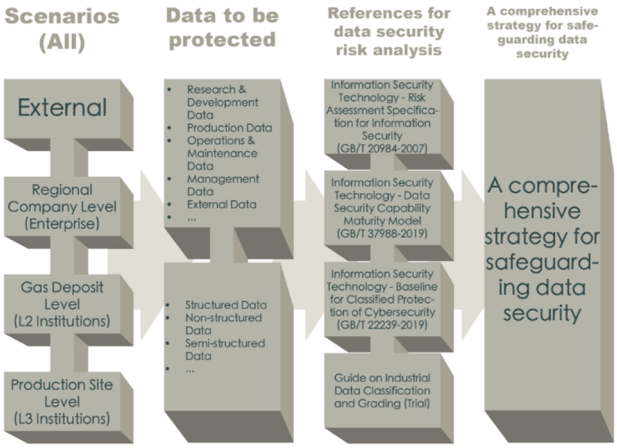

Fig. 1. Design basis of the security protection Strategy framework

(Circular shapes represent the design basis, while rectangular shapes denote design activities.)

In Figure 1, the leftmost depicts the enterprise's four-level application scenario: production site level, gas deposit level, enterprise level and external level. Based on the characteristics of each scenario and its main work content, specific data types are extracted including research and development data, production data, operation and maintenance data, management data and external data. Subsequently, risk analysis is conducted for each type of data according to standards such as the *Information Security Technology—Risk Assessment Method for Information Security* (GB/T 20984-2022) and the *Information Security Technology—Data Security Capability Maturity Model* (GB/T 37988-2019). Finally, security solutions are designed to address these identified risks. Therefore, the mapping sequence between the data life cycle, application scenarios and security attributes can be represented as an M*N multi-dimensional matrix (as shown in Figure 2).

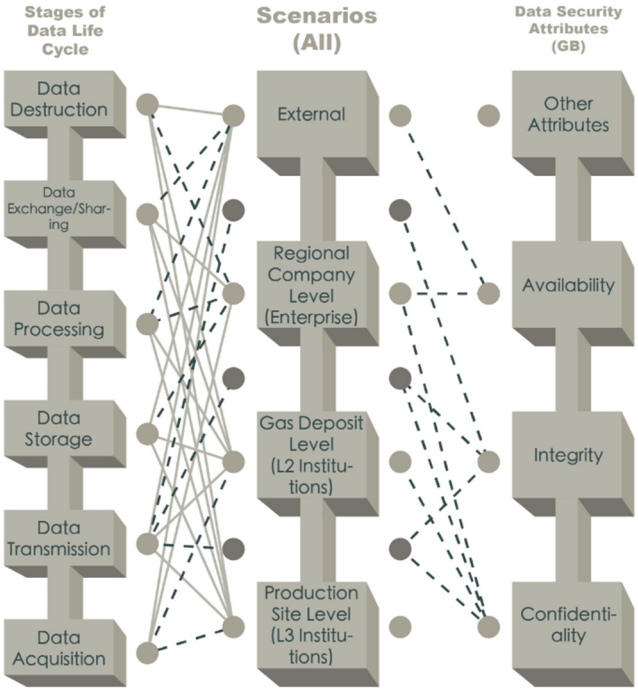

Fig. 2. Relationship between Data Life Cycle and Enterprise Scenarios

The left-hand side of Figure 2 illustrates the life cycle stages of data acquisition, transmission, storage, processing, exchange, and destruction. In the middle section, four application scenarios for enterprise data - production site level (L3 institutions), gas deposit level (L2 institutions), regional company level, and external level - are presented. On the right-hand side is the representation of data security attributes. The lines in the figure on the left indicate potential risks associated with each stage of the data life cycle in their corresponding application scenarios.

3.3 Overall Framework

The data security protection strategy is derived from the business development process and incorporates inputs from legal requirements and obligations, encompassing both managerial and technological dimensions in its approach to safeguarding data. Furthermore, it is imperative for the comprehensive integration of the data security protection strategy throughout all stages of the data life cycle. Figure 3 provides detailed insights into this integration.

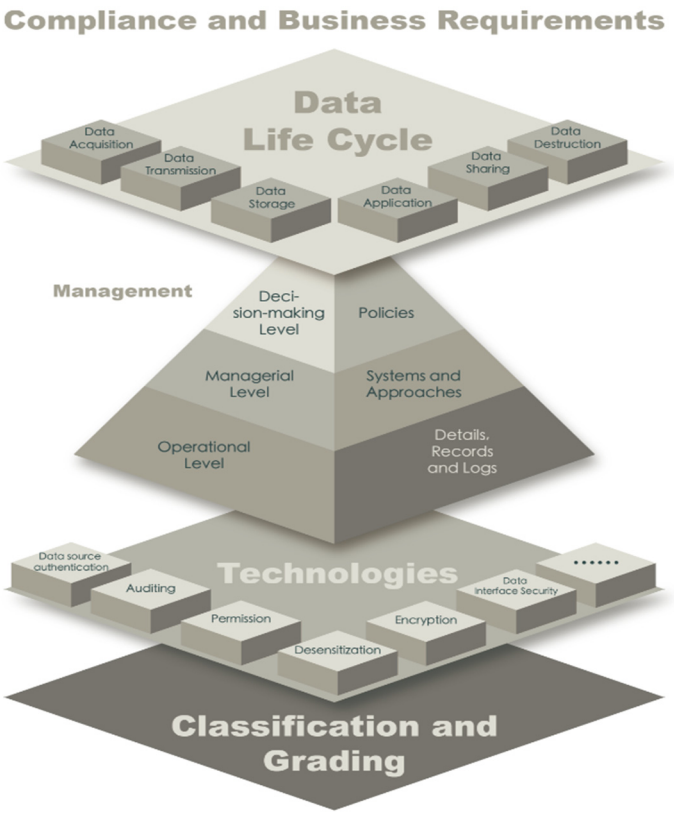

Fig. 3. Flowchart of data security protection Strategy

4 Design of managerial Strategy

Data security management encompasses two dimensions: the organization and the system.

4.1 Data Security Management Organization

The organization of data security management can be divided into three levels: decision-making, managerial, and operational. The decision-making level includes executives involved in business development decisions and decision-makers responsible for data security goals and vision, ensuring a balance between business growth and data security. The managerial level consists of the core entity department responsible for data security as well as business department management, tasked with formulating strategies, plans, and guidelines for data security. The operational level involves personnel from various business departments engaged in data security-related operations and technology implementation to ensure effective execution of measures.

4.2 Data Security Management System

The system process should be comprehensively considered and designed at the enterprise level, forming a systematic framework. It is recommended to refer to the document system structure outlined in the enterprise's *Manual of Comprehensive Management System (Trial version)* and establish three levels of well-structured system documents: first-level documents (policies, general outlines); second-level (management systems, methods, norms); and third-level (operation instructions, detailed rules, forms, reports, various operation/inspection records, log files, etc.).

5 Design of technical strategy

The technical tools involved in all stages of the data life cycle encompass independent system platforms, tools, functions, and algorithm technologies that necessitate holistic consideration during planning and design. Specifically, this entails the integration and connection of general technical tools with the enterprise's business and information systems.

5.1 Overall Technical Framework

Focusing on the data life cycle and targeting data objects and processes, a comprehensive technical framework is designed by selecting appropriate data security techniques and tool platforms, as illustrated in Figure 4.

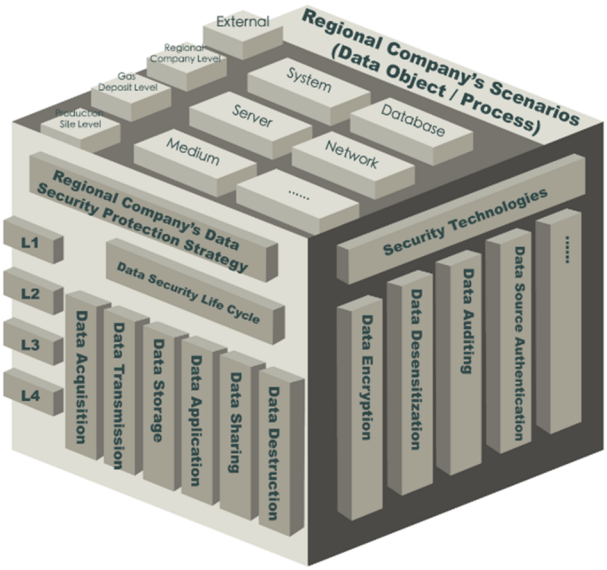

Fig. 4. Architecture diagram of data security technology

5.2 Security Technologies and Products

The data objects and processes that require protection at each stage of the data life cycle, along with common data security technologies and products, are listed in Table 2.

Table 2. The List of data security technologies and products

Stages	Data objects/processes	Security technologies	Safety products
Data Acquisition	Internal systems, external systems, services or applications (such as Web-Service)	Classification and grading labels, data source authentication, etc	Digital watermarking, sensor trusted security detection
Data Transmission	Data synchronization, data migration, terminal transmission, etc	Encryption technology, desensitization technology, etc	Encryptor, data desensitization, data interface machine, application interface service
Data Storage	Databases (online, offline), data warehouses, document storage systems (unstructured data)	Encryption technology, key management, backup and recovery technology, etc	Encryptor, database firewall, vulnerability scanning, anti-virus software, auditing, stored data encryption, database leakage prevention, database auditing and protection, data flow security control, data leakage protection security auditing, file encryption
Data Application	MIS system, analysis and processing platform, document processing platform, data mart (service or product supply)	Encryption technology, desensitization technology, etc	Encryptor, identity authentication and access control, database firewall, intrusion detection, anti-virus software, data desensitization, gatekeeper, data security governance and control platform, database leakage prevention, database auditing and protection, data flow security control, data interface machine, application interface service
Data Sharing	Data sharing/publishing platform	Data interface security, monitoring technology in the process of data sharing	Intrusion detection, auditing, gatekeeper, database auditing and protection, data interface machine, application interface service, trusted protection
Data Destruction	Database, server, hard disk, CD, USB flash drives, floppy disk	Data cleaning and destruction technology, media cleaning and destruction technology	Database firewall, auditing, database auditing and protection

5.3 Design from Data Life Cycle Dimension

Data continuously flows within the enterprise, facilitating business interactions. Throughout this process, these data are also exposed to various security risks. This section proposes effective strategies for safeguarding data security at each stage of its life cycle.

Data Acquisition.

The risks associated with data acquisition primarily manifest at the production site. Site-level operations, process parameters, system logs, and other data are susceptible to

potential threats such as data hijacking, malicious tampering with control instructions, and sensor failures leading to data distortion. These challenges can be effectively addressed through the implementation of a database firewall, digital watermarking, and sensor trusted security detection. Figure 5 illustrates the design of a security protection strategy at the data acquisition stage.

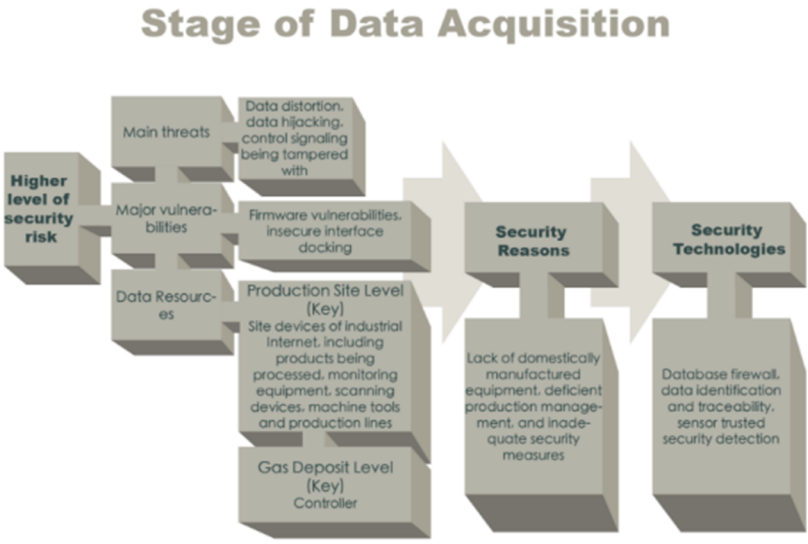

Fig. 5. Design of a security protection Strategy during Data Acquisition

Data Transmission.

Data transmission risks mainly occur at the enterprise level or L2 or L3 institutions of the enterprise. Data related to operations, process parameters, system logs, control information, production operation analysis etc., are transmitted at the gas deposit level, while design data, development and test data, logistics data, system equipment asset information, customer and product information, business statistics and other data at the enterprise level. These transmitted data are exposed to risks such as data being sniffed and data packets intercepted and modified by attackers, which can be solved by de-ploying vulnerability scanning, encryptors, database firewall, identity authentication and access control, and anti-virus software [15-17]. Figure 6 shows the design of a security protection strategy during data transmission.

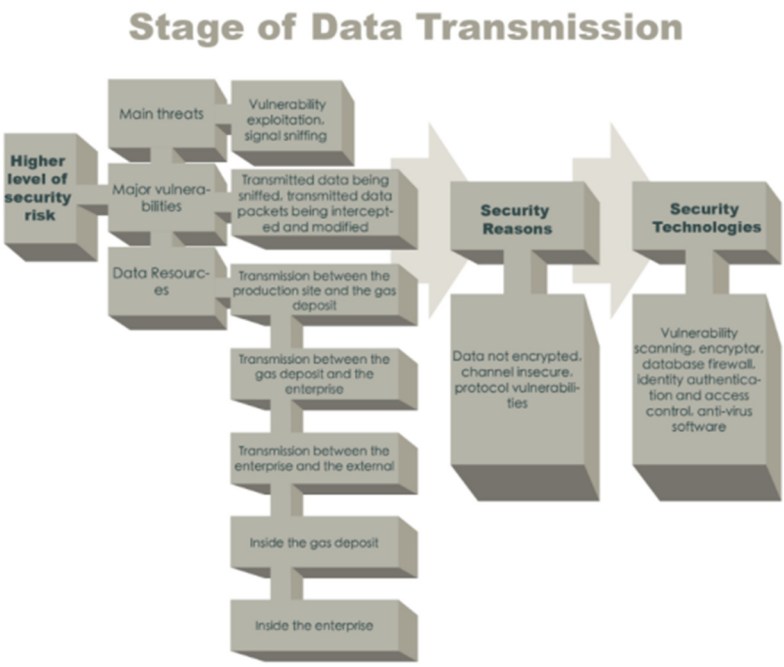

Fig. 6. Design of a security protection Strategy during Data transmission

Data Storage.

The risks associated with data storage primarily manifest at levels of the enterprise and data lake cloud platform. On one hand, the data related to designing, development and testing, geology and engineering, system equipment asset information and business statistics are stored at the enterprise level. On the other hand, the latter is responsible for storing enterprise cloud platform data. These stored datasets face risks such as unauthorized access, sniffing and stealing of stored information, as well as leakage and tampering of cloud platform data. To mitigate these risks effectively during the storage stage, a range of technical products can be deployed including encryptor, database firewall, identity authentication and access control, anti-virus software solutions, intrusion detection (IDS), auditing, stored datasets encryption, digital watermarking, data desensitization, partitioned and segmented storage, and classified and graded storage. Figure 7 illustrates a security protection strategy designed specifically for addressing these concerns.

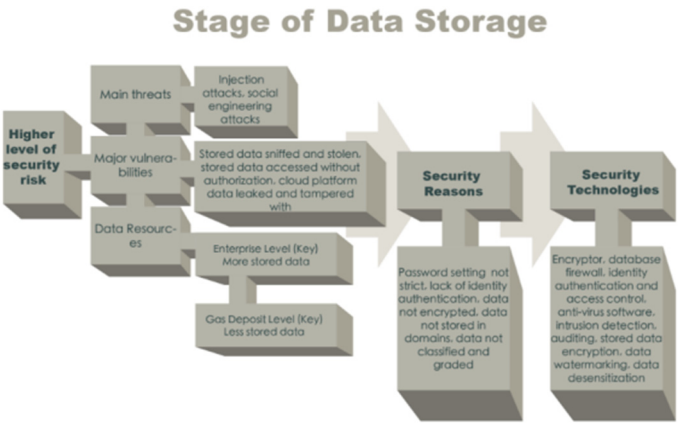

Fig. 7. Design of a security protection Strategy during Data storage

Data Application.

The risks associated with data application primarily manifest at the enterprise level. Data utilized within enterprises encompass designing, development and testing, geology and engineering, system equipment asset information, as well as business statistics. These datasets are susceptible to risks such as unauthorized access or usage, malicious exploitation, data tampering, and inaccurate analysis due to flawed algorithms and models. To mitigate these risks [18-20], security measures can be implemented through the deployment of stored data encryption, identity authentication and access control, along with intrusion detection. Figure 8 illustrates a proposed security protection strategy during data application.

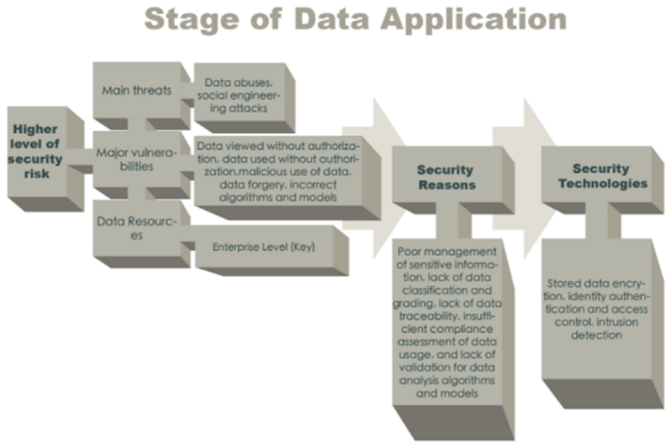

Fig. 8. Design of a security protection Strategy during Data application

Data Sharing.

The risks associated with data sharing primarily manifest at the external level of an enterprise. Data shared outside enterprises are susceptible to risks such as unauthorized exchange and overdue use, which can be effectively mitigated through the implementation of identity authentication and access control, digital watermarking, and data desensitization. Figure 9 illustrates the design of a security protection strategy at the data sharing stage.

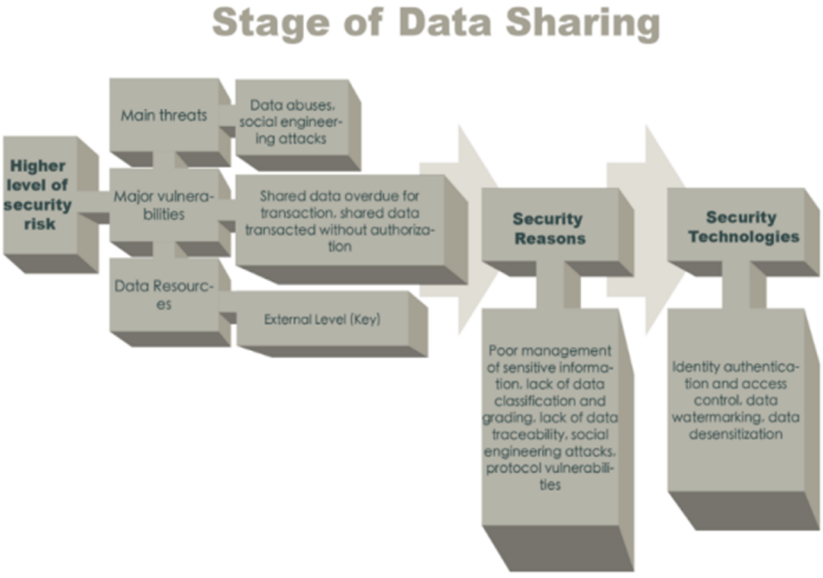

Fig. 9. Design of a security protection Strategy during Data sharing

Data Destruction.

The risks of data destruction primarily occur at the enterprise level. Enterprise-level data of designing, development and testing, geology and engineering, system equipment asset information, business statistics and other types are susceptible to deliberate recovery attempts or incomplete deletion. These risks can be mitigated through measures such as data re-deletion, media destruction, and enhanced security management during the destruction process. Figure 10 illustrates the design of a security protection strategy at the stage of data destruction.

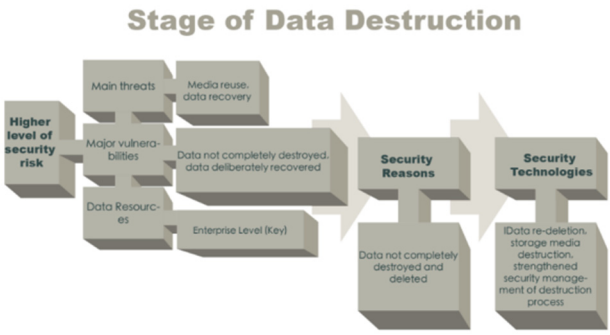

Fig. 10. Design of a security protection Strategy during Data destruction

5.4 Design from Enterprise Scenario Dimension

The scenarios of enterprise data security protection can be categorized into four levels, namely the production site level (L3 institutions), the gas deposit level (L2 institutions), the enterprise level, and the external level, as illustrated in Figure 11. The first two levels correspond to the OT networks of industrial enterprises, while the last two to the IT networks. Certain enterprises deploy edge computing nodes at the OT network site to increase real-time processing of production data. These data is subsequently exchanged with the IT network after desensitization.

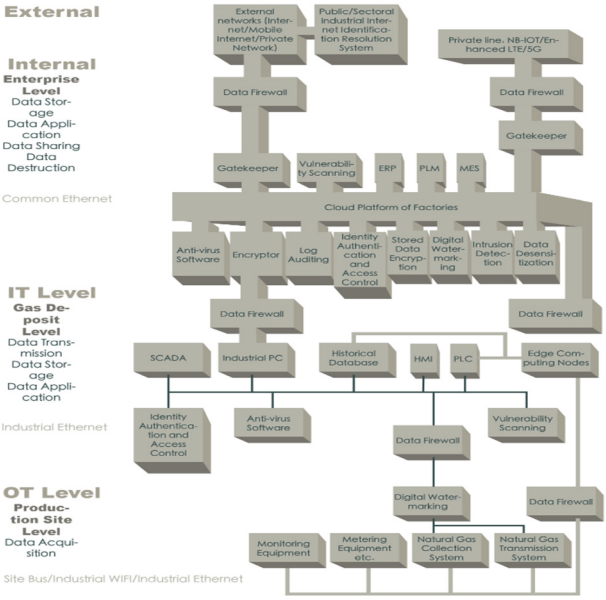

Fig. 11. A general idea for designing a data security strategy at all levels

Production Site Level (L3 Institutions).

The production site level corresponds to the data acquisition stage. At this level, production operation data primarily consists of discrete time series data, which is extensively utilized for geological data analysis, development data management, and production feedback within the enterprise. Consequently, the enterprise places significant emphasis on ensuring high availability, integrity, and real-time nature of production operation data at this level. To mitigate potential security risks faced by these data, lightweight security equipment can be considered as a viable option. Typical risks include hijacking of data, malicious tampering with control instructions, and sensor failures leading to distorted or inaccurate datasets. Figure 12 illustrates the design of a strategy for securing production site data.

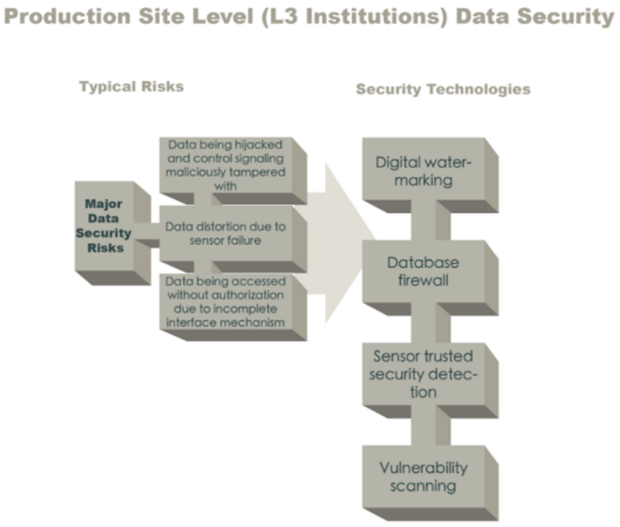

Fig. 12. Design of production site level security protection strategy

Gas Deposit Level (L2 Institutions).

The gas deposit level corresponds to the stages of data transmission, storage, and application. This level primarily pertains to production management data, which is frequently utilized by enterprises for optimizing production models and improving production management methods. Consequently, enterprises place high demands on the confidentiality and availability of gas-deposit-level production management data and can employ lightweight security equipment to mitigate potential risks associated with its security. Typical security risks at this level include sniffing of transmitted data, interception and modification of data packets by attackers during transmission, as well as unauthorized access to the data. Figure 13 illustrates the design of a gas deposit level security protection strategy.

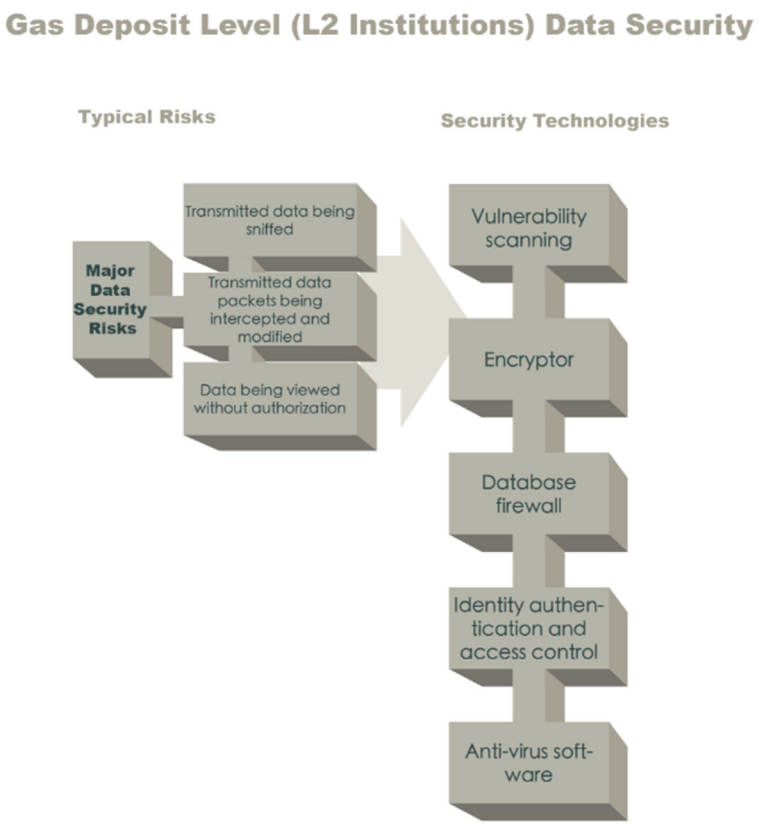

Fig. 13. Design of gas deposit level security protection strategy

Enterprise Level.

The enterprise level also corresponds to the stages of data transmission, storage, and application. This level primarily involves data of development and design, enterprise operation and businesses. These datasets consist of structured, semi-structured, and non-structured formats commonly utilized in enterprise management models and business analysis. Consequently, ensuring the confidentiality, integrity, and availability of these data is crucial. Employing professional security equipment can effectively mitigate potential risks. Typical security risks include unauthorized access or use as well as sniffing or theft of stored information. Figure 14 illustrates a design for safeguarding enterprise level data.

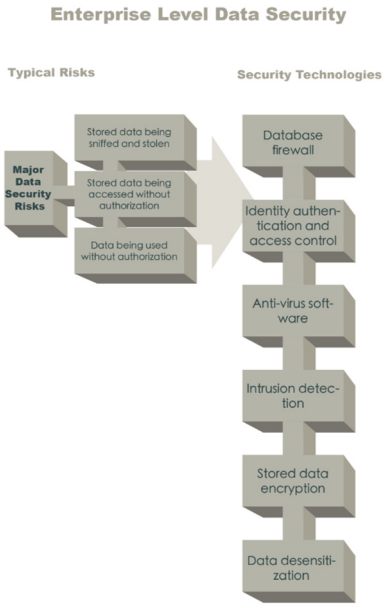

Fig. 14. Design of enterprise level security protection strategy

External Level.

The external level corresponds to the data sharing stage. The main risks at this level are the overdue use and the unauthorized exchange of shared data, which seriously affects the confidentiality and availability. Figure 15 shows the design of an external level data security strategy.

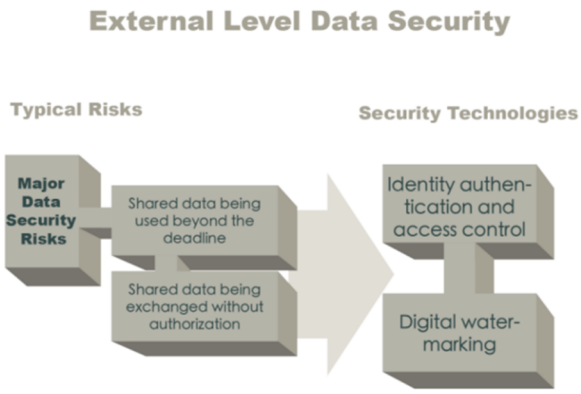

Fig. 15. Design of external level security protection strategy

6 Conclusion

Insufficient data security protection in petrochemical enterprises poses a significant impediment to their digital transformation. To address this issue, it is crucial to expedite research on data security strategies, focusing on both the security management and the technical safeguards, in order to effectively ensure robust data security within these organizations. This paper presents a comprehensive strategy that encompasses the entire life cycle of data, including its acquisition, transmission, storage, application, sharing, and destruction. By considering various dimensions specific to enterprise scenarios and aligning risk analysis with corresponding data security measures at each stage, traditional data security technologies can be integrated into big data platforms to provide enhanced and holistic protection capabilities for enterprise-level data security.

Acknowledgement

This work is supported by the National Key Research and Development Program of China (2020YFB1710000).

References

1. Matturdi B, ZHOU X, LI S, et al. Big Data security and privacy: A review[J]. China Communications, 2014, 11(14): 135-145.
2. WANG W T. Analysis of Computer Network Information Security and Protection Strategy in the Era of Big Data [J]. Science and Information Technology, 2018,000 (025): 67-67.
3. Gao H. Research on Computer Network Information Security and Protection Strategy in the era of Big Data [J]. Science and Technology Innovation, 2018,000 (006): 76-77.
4. ZHANG Y H, SHU J G, YANG K, et al. Scalable and privacy-preserving data sharing based on blockchain[J]. Journal of Computer Science and Technology, 2018, 33(3): 557-567.
5. FENG D G, ZAHNG M, LI II. Big data security and privacy protection[J].Chinese Journal of Computers, 2014, 5 (1): 246-258.
6. Sagiroglu S, Sinanc D. Big data: A review[C]. International Conference on Collaboration Technologies & Systems. 2013.
7. CIIEN II, WANG X X, DUAN Y Q. Analysis and Research on the Value Orientation of Chinese Government's Big Data Policy[J]. Library and Information Service, 2019,64(11):19-27.
8. ZHAO L b, ZHAO K C, HAO S Y. Application of Computer Information Technology in Network Security under the Background of Big Data [J]. Information Technology and Informatization,2019,22(03):89-90.
9. White Paper on Industrial Internet Data Security [Z]. Industrial Information Security Industry Development Alliance. 2020.
10. Lamport L, Shostak R, Pease M. The Byzantine generals problem[M]. Concurrency: the Works of Leslie Lamport. 2019: 203-226.
11. WANG D, ZHAO W B, DING Z M. Analysis and Summary of key technologies of Big Data security [J]. Journal of Beijing University of Technology,2017,43(03):335-349.
12. WANG J H. Discussion on security problems and countermeasures of cloud computing big data [J]. Network Security Technology and Application,2019(11):72-73.

13. RUAN G X. Analysis of Computer network Information security under the background of big data [J]. Computer Products and Distribution,2019(11):38.
14. LI Y J, WANG L H. Research on data security protection strategy under the background of big data [J]. Information and Computer,2020(13):38.184-186.
15. Technology-Energy Technology; Findings from South China Normal University Broaden Understanding of Energy Technology (Positive-temperature-coefficient Graphite Anode As a Thermal RunawayFirewall To Improve the Safety of Licoo2/graphite Batteries Under Abusive Conditions) [J]. Energy Weekly News,2019.
16. Internet and World Wide Web-Internet of Things; Research Conducted at Korea University Has Provided New Information about Internet of Things (Certificate-Based Anonymous Device Access Control Scheme for IoT Environment) [J]. Computers, Networks & amp; Communications, 2020.
17. Citrix Systemsinc.; Researchers Submit Patent Application, "System And Method For Improving Efficiency Of Ssl/Tls Connections", for Approval (USPTO 20190312937) [J]. Computers, Networks& Communications,2019.
18. Wei Kong, Jian Shen, Pandi Vijayakumar, Youngju Cho, Victor Chang. A practical group blind signature scheme for privacy protection in smart grid[J]. Journal of Parallel and Distributed Computing,2020,136.
19. Abdulatif Alabdulatif, Ibrahim Khalil, Xun Yi. Towards secure big data analytic for cloud-enabled applications with fully homomorphic encryption[J]. Journal of Parallel and Distributed Computing,2020,137.
20. Leiyong Guo, Hui Xie, Yu Li. Data Encryption based Blockchain and Privacy Preserving Mechanisms towards Big Data[J]. Journal of Visual Communication and Image Representation,2019.